Journal de Théorie des Nombres
de Bordeaux **18** (2006), 559–572

A Terr algorithm for computations in the infrastructure of real-quadratic number fields

par Johannes BUCHMANN et Ulrich VOLLMER

Dedicated to Michael Pohst on the occasion of his 60^{th} ***birthday.***

Résumé. Nous montrons comment adapter la variante due à Terr de l'algorithme "baby-step giant-step" de Shanks pour le calcul du régulateur et des générateurs des idéaux principaux des corps quadratiques réels. La complexité du pire cas de l'algorithme obtenu dépend uniquement de la racine carrée du régulateur, et est plus petite que toutes celles des algorithmes inconditionnels et déterministes connus précédemment pour ce problème.

Abstract. We show how to adapt Terr's variant of the baby-step giant-step algorithm of Shanks to the computation of the regulator and of generators of principal ideals in real-quadratic number fields. The worst case complexity of the resulting algorithm depends only on the square root of the regulator, and is smaller than that of all other previously specified unconditional deterministic algorithm for this task.

Johannes Buchmann and Ulrich Vollmer
Technische Universität Darmstadt
Department of Computer Science
Hochschulstr. 10, 64289 Darmstadt, Germany
E-mail : {buchmann,uvollmer}@cdc.informatik.tu-darmstadt.de

Manuscrit reçu le 31 décembre 2005.